UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
Case No. 20-cv-954

FARHAD AZIMA,

Plaintiff,

v.

NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC.,

Defendants.

OBJECTIONS OF PLAINTIFF FARHAD AZIMA TO ORDER AND RECOMMENDATION

Magistrate Judge Webster's Order and Recommendation filed on August 9, 2021 (ECF No. 54, "Recommendation") failed to assume the truth of key allegations in the Complaint of Plaintiff Farhad Azima ("Azima") and misinterpreted governing law on several issues. Azima therefore makes the following Objections to the Recommendation for this Court's *de novo* resolution. *See* Fed. R. Civ. P. 72(b)(3).

INTRODUCTION

In 2016, Azima's data, including business records, personal information, privileged documents, trade secrets, and confidential communications, was unlawfully and persistently intercepted in violation of multiple federal and state statutes. Azima believes that this unlawful conduct was instigated by Dechert LLP, Neil Gerrard, RAKIA, and their agents, to injure Azima in a commercial dispute. Azima immediately brought suit for the hacking in the United States against RAKIA and, after that suit was moved to the United Kingdom, he continued to pursue his hacking claims.

In August 2020, Azima learned that Defendants played a principal role in the interception of his data by instructing a company in India to carry out the hack in a way that provided Defendants and their clients, RAKIA and Dechert, with ongoing, real-time access to Azima's electronic communications and other personal and commercial data. After Defendants obtained Azima's intercepted communications, Defendants disclosed the stolen communications to others and used them against Azima. As often occurs in hacking cases, Defendants and their co-conspirators sought to cover their tracks, initially by disguising their identities when sending "phishing" emails to Azima, creating a false paper trail about how they obtained the stolen documents, and using false statements and representations during the litigation.

Within weeks of learning that Defendants committed these violations, Azima brought an eleven-count complaint against them, alleging violations of the Wiretap Act, the trade secrets laws, and various North Carolina laws that provide individuals with causes of action against those who have hacked and intercepted their electronic communications and otherwise invaded their privacy. Defendants moved to dismiss under two theories: The claims were supposedly barred by the relevant statute of limitations and failed to state a claim for relief.

On August 9, 2021, Magistrate Judge Webster recommended that seven of the eleven counts in Azima's Complaint be dismissed and that four counts could proceed to discovery. In the Recommendation, the allegations of trade secret violations, invasion of privacy, and civil conspiracy all survive challenge at this stage of the proceeding.

While the Magistrate Judge recommends dismissal of two of the state law claims on statute of limitations grounds and dismissal of five other counts based on a failure to state claims, the Complaint plausibly states claims that fall within the heartland of the civil recovery provisions of the federal Wiretap Act and the relevant North Carolina tort provisions. Moreover, especially at the pleading stage, the Court should not presume that the statute of limitations has run because the Complaint alleges that Defendants concealed their unlawful conduct and those allegations suffice to defeat the motion to dismiss.

If adopted, the recommendation would make new law in this jurisdiction and make it significantly more difficult for victims of hacking to bring causes of action against those responsible for the hacking, particularly where the hackers conceal their identity. The recommendations would also alter the legal landscape and significantly narrow the available causes of action for victims of hacking. For the reasons discussed in more detail below, this Court should reject the recommendations to dismiss Counts I, II, IV, V, VI, VII and IX, accept the other recommendations, and allow the entire case to proceed.

OBJECTIONS

I. Azima's Complaint Sufficiently Pleads Wiretap Act Claims.

The Magistrate Judge incorrectly recommends dismissal of the two Wiretap Act counts in the Complaint. The first Wiretap Act count (Count I) alleges that Defendants used and disclosed Azima's data, and the second Wiretap Act count (Count II) alleges that Defendants procured the unlawful "intercept" of the data. As discussed below, both the disclosure and use of the intercepted data and the procurement of the intercept are violations of the statute. In addition, the civil liability provision of the Wiretap Act (18

U.S.C. § 2520) creates a private cause of action for Azima, the person whose data was intercepted. The Recommendation regarding this issue is flawed because it is based upon a misreading of the plain text of the statute and the Magistrate Judge did not properly consider the express content of Azima's Complaint.

The Wiretap Act was passed by Congress in 1968 to address illegal wiretapping – *i.e.*, the interception of written or oral communications by the government or by private individuals without authorization or consent. *See generally* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90 -351, tit. III, 82 Stat. 197(codified at 18 U.S.C.§§ 2510 -2522).[1] Section 2511(1) of the Wiretap Act makes it a violation to intercept, endeavor to intercept, or "procure[] any other person to intercept" any wire, oral, or electronic communication; to disclose or endeavor to disclose any intercepted communication; and to use or endeavor to use any intercepted communication.

Section 2520(a) provides that a civil claim under the statute can be brought by "any person whose wire, oral, or electronic communication is intercepted, disclosed or intentionally used in violation of this chapter " against "the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate."[2] This section creates a private cause of action for a person whose communications *were*

[1] The Wiretap Act was revised in 1986 as part of the Electronic Communications Privacy Act (ECPA) to include electronic communications in addition to wire and oral communications. *See generally Joffe v. Google, Inc.*, 746 F.3d 920, 935 (9th Cir. 2013) (discussing congressional changes to resolve internal tensions in the Wiretap Act).

[2] The civil remedy contains exceptions for phone carriers and law enforcement agencies that are not relevant here.

intercepted, disclosed or used in violation of the Wiretap Act to sue any person or entity that "engaged in that violation." *See Boseovski v. McCloud Healthcare Clinic, Inc.*, No. 2:16-CV-2491-DMC, 2020 WL 68578, at *6 (E.D. Cal. Jan. 7, 2020).

Azima makes numerous allegations that he was the victim of a violation of the Wiretap Act when his communications were "intercepted," "disclosed," and used in violation of the Wiretap Act, and those allegations support a private cause of action under section 2520. *See, e.g.*, Compl., ECF No. 1, ¶¶ 6, 16-18, 19, 22. As a result, Azima may sue any person or entity that "engaged in that violation" of the Wiretap Act. The Complaint alleges that Defendants "engaged in that violation." The Complaint further alleges that Defendants violated 18 U.S.C. § 2511(1)(c) (prohibiting unlawful disclosure of communications intercepted in violation of the Wiretap Act) **and** 2511(1)(d) (prohibiting unlawful use of communications "intercepted" in violation of the Wiretap Act) **and** 2511(1)(a) (making it unlawful for "any person" to "procure[] any other person to intercept" data in violation of the Wiretap Act). ECF No. 1 ¶¶ 1, 48, 55, 92, 93, 95, 110. Therefore, Azima may sue Defendants under the Wiretap Act under all of these theories.

Intentional Disclosure of Intercepted Communications: 18 U.S.C. § 2511(1)(c) prohibits intentional disclosure of communications intercepted in violation of the Wiretap Act if the person knows or has reason to know that the communications were intercepted It is not in dispute that Defendants knew that Azima's stolen emails were intercepted, and the Complaint clearly alleges that Defendants disclosed Azima's stolen data. *See* Compl., ECF No. 1, ¶ 48 ("Defendants Del Rosso and Vital intentionally disclosed wire and electronic communications of Azima knowing and/or having reason to know that the

information was obtained through interception."); ¶ 92 ("Defendants knowingly broadcast or published personal information of Azima on the internet with actual knowledge that Azima objected to any such disclosure and without Azima's consent or knowledge."); ¶ 93 ("Defendants published Azima's private information on blog sites hosting WeTransfer links in May and June of 2018, and again in June of 2019."); ¶ 95 ("Defendants published financial transaction records, spreadsheets, business records, and banking information, all of which were and are marked confidential.").

Moreover, Defendant Del Rosso admitted in a sworn witness statement filed in a U.K. court (as discussed in Azima's Complaint and as contained in the record of this case) that he disclosed Azima's stolen data by emailing links to the intercepted data and by personally flying to New York with a thumb drive containing the intercepted data to hand deliver it to Neil Gerrard of Dechert LLP. *See* ECF No. 25-3 ¶¶ 10, 14, 16; *see also* ECF No. 34 at 15 n.3. These allegations are more than adequate to state a claim under the Wiretap Act. *See, e.g.*, *Doe v. Smith*, 429 F.3d 706, 709 (7th Cir. 2005); *Nalley v. Nalley*, 53 F.3d 649, 650 (4th Cir. 1995); *Lewton v. Divingnzzo*, 772 F. Supp. 2d 1046, 1060 (D. Neb. 2011).

Intentional Use of Intercepted Data: Similarly, 18 U.S.C. § 2511(1)(d) makes it a violation of the Wiretap Act to intentionally "use" intercepted communications. As described above, *see* Compl., ECF No. 1, ¶¶ 48, 92, 93, 95 the Complaint plausibly alleges a theory of unlawful "use" in violation of the Wiretap Act, describing both the use of the data by Defendants and Defendants' knowledge of the unlawful intercept. *See Lewton*, 722 F. Supp. 2d at 1058; *Leach v. Bryam*, 68 F. Supp. 2d 1072, 1074-75 (D. Minn. 1999).

Procurement of the Intercept: Finally, 18 U.S.C. § 2511(1)(a) makes it a violation of the Wiretap Act for any person to "intentionally intercept[], endeavor[] to intercept, *or procure[] any other person to intercept or endeavor to intercept*, any wire, oral, or electronic communication." *Id*. (emphasis added). The Complaint alleges that Defendants "procured" the interception of Azima's communications by hiring a hacking firm to intercept those communications and paying for the intercept, and Defendants agree that these allegations are in the Complaint. *See* ECF No. 1. ¶¶ 55-58; ECF No. 32 at 17-18. Azima has therefore made sufficient allegations to withstand a motion to dismiss based on Defendants having "engaged in that violation." 18 U.S.C. § 2520 (a). "[B]oth the person who actually intercepted the communications and the person who procured the interception have violated the Act, and the victim is authorized to sue any person or entity who engaged in that violation." *Lonegan v. Hasty*, 436 F. Supp. 2d 419, 428 (E.D.N.Y. 2006); *see also Boseovski v. McCloud Healthcare Clinic, Inc.*, No. 2:16-CV-2491-DMC, 2020 WL 68578, at *6 (E.D. Cal. Jan. 7, 2020).

Errors in the Recommendation: The Recommendation states that Azima's allegations of disclosure of hacked data lack particularity. Yet the Complaint makes multiple allegations that Defendants disclosed intercepted data and knew that it was unlawfully intercepted because Defendants procured the interception. These allegations sufficiently alleged a plausible theory of unlawful disclosure in violation of the Wiretap Act. This Court should therefore reject the recommendation to dismiss Count I.[3]

[3] To the extent the Court determines that Azima's Complaint did not include sufficient facts of disclosure or use, the proper remedy is to dismiss with leave to amend, not to dismiss with prejudice, particularly given the clear admissions in Defendant Del

The Recommendation also ignored the plain language of the Wiretap Act in finding that procurement of an unlawful intercept is not actionable. Section 2520 provides that the plaintiff can sue anyone who is "engaged in that violation." *Id.*[4] By ignoring this clear statutory language, the Recommendation violated the first canon of statutory interpretation: The "language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case." *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340 (1997). And "the statutory language is unambiguous and 'the statutory scheme is coherent and consistent.'" *Id.; see also Connecticut Nat. Bank v. Germain*, 503 U. S. 249, 253-54 (1992). Because the text of § 2511(1)(a) clearly says that procurement of an unlawful intercept is a violation of the statute, that should have been the end of the inquiry.

Rather than examine the text of § 2511(1)(a), the Magistrate Judge focused on a perceived difference between the original text of § 2520 and the version of § 2520 as amended in 1986. The original text stated that any person whose communications were

---

Rosso's witness statement that he emailed links to Azima's intercepted data and then flew with copies of Azima's intercepted data to hand deliver copies to Dechert. *See Laber v. Harvey*, 438 F.3d 404, 426 (4th Cir. 2006) (en banc) (holding that "Rule 15(a) directs that leave to amend 'shall be freely given'" to give effect to "the federal policy in favor of resolving cases on their merits instead of disposing of them on technicalities."). However, amendment is not necessary in this case given the allegations in the Complaint and plausible inferences that result therefrom, and requiring amendment is both unnecessary and would further delay this litigation, which has been pending for 10 months.

[4] Instead, the Magistrate Judge appears to have concluded incorrectly that Azima alleges "secondary" or "aiding and abetting" liability, and then determined (based on case law from other jurisdictions) that Section 2520 does not authorize this form of "secondary" liability. *See* ECF No. 54 at 18 (citing *Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1246 (10th Cir. 2012); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 169 (5th Cir. 2000)). The Complaint alleged primary, not secondary, liability because it alleged that Defendants violated the Wiretap Act by procuring the intercept of Azima's data, which is a violation of Section 2511(1)(a).

intercepted, used, or disclosed had a civil remedy "against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications." *Id.* With this change, Congress broadened the applicability of the statute by eliminating the more specific definition of the proper defendant and instead providing a catch-all remedy against any person or entity who "engaged in that violation." *See, e.g.*, *Fourco Glass Co. v. Transmirra Products Corp*., 353 U.S. 222, 227 (1957) (noting that "no changes of law or policy are to be presumed from changes of language in the revision unless an intent to make such changes is clearly expressed") (footnote omitted)*; Robert E. Lee & Co. v. Veatch*, 301 F.2d 434, 437-38 (4th Cir. 1961) ("At most, the statute is ambiguous . . . it will not be inferred that Congress, in revising and consolidating the laws, intended to change their effect unless such intention is clearly expressed.").

As the court noted in *Lonegan*, a review of the legislative history of Section 2520 shows that Congress was silent concerning the changes despite "explain[ing] most of the statutory changes . . . in meticulous detail," which supports the natural reading of the statute and suggests that Congress intended to make non-substantive changes to the statute. *See Lonegan*, 436 F. Supp. 2d. at 428; *see also Boseovski*, 2020 WL 68578, at *6 ("Given that procurement can still give rise to a violation under § 2511(1)(a), and given that an entity may be civilly liable under § 2520(a) for that violation, defendant in this case may be held civilly liable if it violated the underlying criminal statute by way of procurement."). A plain reading of the statutory language demonstrates that Azima has a valid cause of action against Defendants for procuring the interception.

Because the Complaint alleges that Defendants hired and paid CyberRoot to hack Azima's computers and that Defendants disclosed and used Azima's intercepted data, knowing it was obtained through interception, the Court should reject the recommendation to dismiss Counts I and II.

II. Azima Adequately Pleaded All of His State Law Claims.

The Magistrate Judge recommended dismissing Azima's state law claims for computer trespass (Count IV), conversion (Count V), identity theft (Count VI), publication of personal information (Count VII), and violation of the North Carolina Unfair and Deceptive Trade Practices Act (Count IX). ECF No. 54 at 3-4. Azima respectfully objects to these recommendations and requests that Defendants' motion to dismiss Azima's state law claims be denied.

A. Defendants Are Equitably Estopped from Asserting the Statute of Limitations Because They and Their Co-Conspirators Concealed Their Identity and Conduct from Azima.

The Magistrate Judge recommended dismissing Azima's state law claims for computer trespass (Count IV) and conversion (Count V) because he concluded that the Complaint does not "establish the element of reliance that is necessary to invoke the North Carolina doctrine of equitable estoppel to preclude application of the statute of limitations to his computer trespass and conversion claims." ECF No. at 15. This recommendation should be rejected.

Under North Carolina law, the doctrine of equitable estoppel bars Defendants from asserting the statute of limitations if they concealed their identity from Azima. *See Friedland v. Gales,* 509 S.E.2d 793, 797 (N.C. App. 1998). The Complaint alleges that Del

Rosso and his co-conspirators concealed his and their identity from Azima and that Azima did not discover Defendants' involvement in the hacking conduct until "recently." *See* Compl., ECF No. 1 ¶ 36.

In *Friedland*, the plaintiff sued the defendant for wrongful death more than two years after the death of the victim. *Friedland*, 509 S.E.2d at 794-95. Even though plaintiff asserted that his delay in filing was because the defendant denied killing the victim, the trial court dismissed the plaintiff's claims based on the two-year statute of limitations, *id.* at 795. The North Carolina Court of Appeals overturned the lower court and held that the suit was timely because equitable estoppel barred the statute of limitations defense. *Id.* at 798. The Court held that "one who actively, affirmatively and deliberately conceals his identity as a tortfeasor is equitably estopped from asserting the statute of limitations as a defense to an action for damages resulting from his tortious act." *Id.* at 796. The Court explained that even though "the actual injury was known and the claim had accrued . . . due to defendant's intentional concealment, an essential fact necessary to bring the action, i.e., the identity of the tortfeasor was unknown." *Id*. at 798. Thus, the Court reasoned that:

> Plaintiff, lacking the reasonable means to discover the identity of the wrongdoer, reasonably relied on the concealment to his detriment by not filing a wrongful death action until such information became available to him. These findings of fact establish, as a matter of law, that defendant, having actual knowledge of material facts, actively and deliberately concealed those facts with the intent to prevent discovery thereof by others, including the plaintiff; and that in consequence of defendant's conduct, plaintiff was without knowledge of those facts and without means to discover them within the period of the statute of limitations, thereby relying to his detriment on defendant's conduct.

Id.

In addition, statements by related parties that conceal the identity of the tortfeasors can estop defendants from raising a statute of limitations defense. In *Hatcher v. Flockhart Foods, Inc.*, the North Carolina Court of Appeals found that a defendant—the lessee of a store in which the plaintiff was injured—was equitably estopped from asserting the statute of limitations because the defendant's insurer concealed the identity of the defendant and the insurer's concealment was then imputed to defendant. *Hatcher v. Flockhart Foods, Inc.*, 589 S.E.2d 140, 142 (N.C. App. 2003). In that case, the plaintiff fell in a grocery store and plaintiff's counsel sent a letter to the grocery store's corporate office. *Id.* at 141. The grocery store's insurer responded to plaintiff's counsel, but never informed plaintiff's counsel that the grocery store contacted by plaintiff's counsel had leased the property to defendant, even though the insurer insured the grocery store *and* the lessee-defendant. *Id.* at 141, 143. The Court held that the defendant was equitably estopped from asserting the statute of limitations because "[a]fter viewing the evidence in the light most favorable to plaintiff, we can conclude that plaintiff lacked knowledge that [defendant] was the proper defendant to sue and was unable to discover that knowledge because the lease between [defendant] and [the grocery store] was not recorded in the Register of Deeds office" and "Plaintiff relied on correspondence between he and the insurer that indicated that [another corporate entity] was the insured." *Id.* at 143.

Here, the Complaint alleges that Azima was hacked through spear-phishing emails, which are inherently deceptive and disguised the identity of those who conspired to hack Azima. Compl., ECF No. 1, at ¶ 6. The phishing "campaign" cost more than $1 million and "lure[d]" Azima to "unwittingly" provide his credentials. *Id.* at ¶¶ 6, 16, 17. The

campaign gave Defendants and their co-conspirators persistent access Azima's data, which shows inherent ongoing deception about identity of those involved with the hack. *Id*. These allegations from the Complaint make clear that Defendants sought to conceal their identities and their role in the hacking since the beginning, and that concealment has continued to this day.

The Complaint also explicitly alleges that "Page, Del Rosso, Gerrard, and RAKIA's manager James Buchanan created a false evidentiary trail to cover up their and RAKIA's responsibility for hacking, and to suggest that Page had innocently found the hacked material on BitTorrents." ECF No. 1 ¶ 7. The Complaint also alleges that "CyberRoot posted the [stolen] data on the internet to create the misimpression that the data CyberRoot and Defendants stole from Azima were available to anyone who used the internet," and "Page, Del Rosso, Gerrard, and an Israeli journalist, Majdi Halabi, created a false story and evidentiary trail to cover up their and RAKIA's responsibility for the hacking, and to suggest that Page had innocently found the hacked material on BitTorrents after being alerted to it by Halabi." *Id*. ¶ 22.

In addition, Defendants' co-conspirators repeatedly denied (in court proceedings in the US and the UK) hacking Azima and made false representations that were designed to conceal, in large part, Defendants' role in the hacking. At the U.K. trial, Defendants' co-conspirators RAKIA, Dechert, Gerrard, Buchanan, and Page were untruthful about how they obtained Azima's stolen data, and the English court ultimately found that "the true facts" had not been disclosed. *Id*. ¶ 34. "Del Rosso was an important part of RAKIA's false story of 'innocent discovery' by Page of Azima's stolen data" and "[t]he emails of August

15 and 16, 2016, between Gerrard and Del Rosso were clearly an attempt to lay a false 'paper trail' of discovery." *Id.* ¶ 35. Finally, Azima alleges that "Del Rosso hid his engagement of CyberRoot and denied any involvement in the hacking." *Id.* ¶ 36. "Because of Del Rosso's concealment of the true facts, of which he had knowledge, Azima did not learn of the role played by Del Rosso and Vital until recently." *Id.*[5]

Based on these allegations, Defendants should be equitably estopped from asserting the statute of limitations, especially at the pleading stage where Azima's allegations must be taken as true and Azima need only allege facts sufficient to raise a plausible inference. *See Bankaitis v. Allstate Ins. Co.*, 229 F. Supp. 3d 381, 387 (M.D.N.C. 2017) (finding that Plaintiffs alleged sufficient facts to state a plausible claim for equitable estoppel even though plaintiffs "failed to allege misrepresentations by [defendant] that caused plaintiffs to delay bringing suit" because Plaintiffs alleged they relied on defendant's concealment of its intent to deny coverage); *Friedland*, 509 S.E.2d at 798 ("Generally, where there are facts in dispute as to the existence of the elements of equitable estoppel, the issue of estoppel is for the jury."); *Miller v. Talton*, 435 S.E.2d 793, 797 (N.C. App. 1993) ("If the evidence in a particular case raises a permissible inference that the elements of equitable estoppel are present, but other inferences may be drawn from contrary evidence, estoppel is a question of fact for the jury."); *accord Goodman v. Praxair, Inc.*, 494 F.3d 458, 464 (4th Cir. 2007) ("[A] motion to dismiss filed under Federal Rule of Procedure 12(b)(6),

[5] In the US litigation brought by Azima against RAKIA, RAKIA also denied involvement in the hacking.

which tests the sufficiency of the complaint, generally cannot reach the merits of an affirmative defense, such as the defense that the plaintiff's claim is time-barred.").

B. Azima's Allegations Support an Inference that Defendants Used Azima's Identifying Information to Steal Azima's Confidential Information and Trade Secrets.

As demonstrated in Azima's Complaint, the essence of a phishing hack is that hackers conceal their identity from the victim, obtain the victim's identifying information (such as passwords and usernames), and then use that identifying information to pose as the victim to steal their data. By seeking and obtaining Azima's passwords and using them to gain repeated and persistent access to Azima's email accounts, Defendants committed identity theft against Azima, and the recommendation to dismiss Count VI should be rejected.

"A person who knowingly obtains, possesses, or uses identifying information of another person, living or dead, with the intent to fraudulently represent that the person is the other person . . . to obtain anything of value, benefit, or advantage . . . is guilty of a felony." N.C. Gen. Stat. § 14-113.20(a) (2005). "The term 'identifying information . . . includes . . . passwords." *Id.* § 14-113.20(b)(13). And "any person who commits an act made unlawful by Section 14-113.20 [] may be liable for damages under [Section] 1-539.2C." N.C. Gen. Stat. § 14-113.22(b). The Magistrate Judge recommended dismissing Azima's state law identity theft claim because he could not "identify specific factual allegations in the complaint demonstrating that Defendants made representations to any other individual or entity that they were Plaintiff." Recommendation at 26. This recommendation should also be rejected because, by defining "identifying information" to

include "passwords," the statute clearly contemplates that logging into Azima's account using his stolen usernames and passwords is a misrepresentation that Defendants were Azima. This conduct is clearly alleged in the Complaint. ECF No. 1 at ¶¶ 4, 6, 89, 90.

"[T]he appellate courts of [North Carolina] have long recognized that fraudulent intent in various financial crimes need not be shown by verbal misrepresentation, but can also be established based upon a defendant's conduct or actions." *State v. Jones*, 734 S.E.2d 617, 621 (2012), *affirmed by State v. Jones,* 758 S.E.2d 345, 350 (2014). In *Jones,* the North Carolina Court of Appeals held that "implicit misrepresentations by conduct" satisfied the intent requirement for identity theft. *Id.* at 622. In that case, the evidence showed the defendant possessed other people's credit card information and had possession of items purchased with those credit cards. *Id.* The Court held that this evidence "would support a reasonable inference by the jury that Defendant fraudulently used credit card numbers belonging to other people without authorization to make purchases and payments on his own behalf." *Id.* The Court added that "[n]o verbal statement of one's identity is required[.]" *Id.*

Azima alleges similar "implicit misrepresentations by conduct" in this case. Specifically, Azima alleged that:

> At the direction of Del Rosso, Vital, and others, CyberRoot sent Azima phishing emails asking him to reset his password. Azima complied, and unwittingly permitted CyberRoot's hackers to gain access to Azima's email accounts and computers. The persistent access to Azima's email accounts and computers allowed CyberRoot, at the direction of Defendants Del Rosso and Vital, to use Azima's email addresses and passwords to obtain substantial quantities of Azima's private data, including trade secrets, confidential

> business information, and personal information and communications.

Compl., ECF No. 1, ¶ 90.

Azima also alleges that "at least some of [the data obtained by CyberRoot] was provided to Del Rosso," *id.* ¶ 19, and "Del Rosso, Vital, CyberRoot, and other co-conspirators, including Dechert LLP, Gerrard, and Page, obtained numerous confidential and protected trade secrets belonging to Azima and his companies, including but not limited to privileged and confidential legal communications and advice and confidential internal pricing lists relating to food transport for U.S. troops in Afghanistan." *Id.* ¶ 18. Thus, as in *Jones*, Azima's allegations that Defendants had access to Azima's passwords through CyberRoot, and possessed confidential information and trade secrets (*i.e.*, things of value, benefit, and advantage) obtained from accounts protected by those passwords. These allegations support a plausible inference that Defendants implicitly represented themselves to be Azima by using his passwords to secure access to his accounts, thereby committing identity theft.

C. Azima Objected to the Publication of His Personal Information by Marking the Documents as Confidential and by Bringing Claims Against RAKIA in U.S. and U.K. Lawsuits Prior to the Publication of the Data in 2019.

The Magistrate Judge recommended dismissing Azima's claim for publication of personal information (Count VII) because he concluded that Azima did not allege that he objected to the publication of stolen and confidential information before Defendants published the data online. Recommendation at 26-27. This recommendation once again fails to consider all the allegations in the Complaint, including Azima's allegation that "Defendants knowingly broadcast or published personal information of Azima on the

internet with actual knowledge that Azima objected to any such disclosure and without Azima's consent or knowledge," Compl., ECF No. 1, ¶ 92. Because the recommendation did not make plausible inferences in favor of Azima, the Court should reject the Recommendation for the following two reasons.

First, Azima alleges the documents published by Defendants included "financial transaction records, spreadsheets, business records, and banking information, ***all of which were and are marked confidential.***" *Id.* ¶ 95 (emphasis added). Azima also alleges that he took reasonable measures to keep his information secret, including maintaining information on a secure server protected by passwords. *Id.* ¶ 66. Indeed, Defendants phished Azima to steal his passwords and access his accounts without his consent, which would not have been necessary if Defendants did not know that Azima objected to the publication of his confidential data.

Second, Azima objected to the publication of his data in the strongest way – by suing RAKIA for its acts and the acts of its agents for the hack and publication of his stolen data. The publication of Azima's stolen data continued after Azima raised this public objection. Indeed, some of the hacked data was published after that suit was filed. Azima alleges that CyberRoot—at Defendants' direction—modified websites and published his stolen data in 2018 and 2019. *Id.* ¶¶ 24-26, 49. This Court can thus plausibly infer that Defendants knew in 2018 and 2019 that Azima objected to disclosing his stolen data because Azima defended the claims in the U.K. lawsuit by claiming RAKIA stole his data. *Id*. ¶ 7. And even though Defendants were not parties to the U.K. lawsuit, Azima alleges that (1) Del Rosso was hired by Dechert and RAKIA to steal the data that was used in the

lawsuit, *id.* ¶ 2; (2) Del Rosso emailed with RAKIA's counsel in August 2016 about the hacked materials to create a false paper trail, which would have been unnecessary if Azima did not object to the publication,[6] *id.* ¶ 35; and (3) Del Rosso testified (falsely) in the English lawsuit, *id.* ¶ 36. Thus, this Court can plausibly infer that Defendants knew of Azima's ongoing lawsuits and therefore also knew of his repeated objection before the publication of the data in 2018 and 2019.

D. The Complaint Properly Alleges a Violation of the North Carolina Unfair and Deceptive Trade Practices Act.

The Magistrate Judge recommended dismissing Azima's claim for violating North Carolina's Unfair and Deceptive Trade Practices Act ("UDTPA") because "[t]he complaint does not contain any allegation that Plaintiff was engaged in commercial dealing with Defendants or that Plaintiff's companies and Vital are competitors . . . [n]or has Plaintiff alleged that the deceptive acts by Defendants have negatively affected the consuming public." Recommendation at 30.[7] This analysis is flawed and the recommendation should be rejected by this Court.

[6] Although the Magistrate Judge discounted Azima's allegation about a false paper trail, *see* ECF No. 54 at 15, the Court must take the allegations as true at this stage.

[7] The Magistrate Judge did not address Defendants' argument that Azima's UDTPA claim failed because Azima did not allege an unfair or deceptive trade practice. ECF No. 32 at 34. Defendants' argument has no merit because, among other reasons, the Magistrate Judge found that Azima alleged a claim for misappropriation of trade secrets and "[a] violation of the Trade Secrets Protection Act constitutes an unfair act or practice under N.C. Gen. Stat. § 75–1.1." *See, e.g.*, *Med. Staffing Network, Inc. v. Ridgway*, 670 S.E.2d 321, 329 (N.C. App. 2009).

For purposes of the UDTPA, "'commerce' includes all business activities, however denominated." N.C. Gen. Stat. § 75-1.1(b) (1977). Commerce includes many types of commercial relationships, "including those outside of contract." *Prince v. Wright*, 541 S.E.2d 191, 196 (N.C. App. 2000). Furthermore, "[i]f a party engages in conduct that results in an inequitable assertion of his power or position, he has committed an unfair act or practice." *Johnson v. Beverly-Hanks & Assocs., Inc.*, 400 S.E.2d 38, 42 (N. C. App. 1991).

The Complaint alleges that Del Rosso owns Vital and "Vital purports to provide investigative services." Compl., ECF No. 1, ¶ 11. RAKIA[8] hired Gerrard and Dechert LLP, who hired Defendants to hack Azima and steal his data. As alleged by Azima, "Defendants, CyberRoot, Dechert LLP, and Page engaged in this conspiracy pursuant to a common scheme of damaging Azima and tarnishing his reputation," *id.* ¶ 135, and Azima "suffered harm to business relationships," *id.* ¶ 134. Azima's allegations therefore support a plausible inference that the conduct of Defendants and their co-conspirators constituted deceptive and unfair practices that "affected commerce."

[8] Although it was not alleged in the Complaint, Azima and RAKIA were former business partners as has been discussed multiple filings in federal and U.K. courts. The Complaint adequately alleges commerce, as discussed above. Azima could amend his Complaint to specifically make this allegation, *see Laber*, 438 F.3d at 426, but doing so is not necessary and would only serve to delay this litigation, which was filed ten months ago.

CONCLUSION

For the foregoing reasons, Azima respectfully requests that the Court reject the Recommendation with respect to Counts I, II, IV, V, VI, VII, and IX, accept the other recommendations, and deny Defendants' motion to dismiss.

This, the 23rd day of August, 2021.

WOMBLE BOND DICKINSON (US) LLP

/s/ Ripley Rand
Ripley Rand
North Carolina Bar No. 22275
Christopher W. Jones
North Carolina Bar No. 27625
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: ripley.rand@wbd-us.com
chris.jones@wbd-us.com

MILLER & CHEVALIER CHARTERED

/s/ Kirby D. Behre
Kirby D. Behre (*pro hac vice*)
Brian A. Hill (*pro hac vice*)
Tim O'Toole (*pro hac vice*)
Ian Herbert (*pro hac vice*)
Calvin Lee (*pro hac vice*)
900 16th Street, NW
Washington, D.C. 20006
Telephone: (202) 626-5800
Fax: (202) 626-5801
Email: kbehre@milchev.com

Counsel for Plaintiff

CERTIFICATE OF WORD COUNT

I certify under LR 7.3(d)(1) and LR 72.4 that the body of this objection, headings, and footnotes together contain 6,250 words or fewer, as reported by the word count feature in Microsoft Word 2016.

WOMBLE BOND DICKINSON (US) LLP

/s/ *Ripley Rand*
Ripley Rand
North Carolina Bar No. 22275
Christopher W. Jones
North Carolina Bar No. 27625
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: chris.jones@wbd-us.com
ripley.rand@wbd-us.com

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO. 20-CV-954

FARHAD AZIMA,

Plaintiff,

v.

NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC.,

Defendants.

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send electronic notification of this Notice to the following attorneys:

Kieran J. Shanahan, Esq.
Brandon S. Neuman, Esq.
Jeffrey M. Kelly, Esq.
Nathaniel J. Pencook, Esq.
GlenLake One
4140 Parklake Avenue - Suite 200
Raleigh, NC 27612
kieran.shanahan@nelsonmullins.com
brandon.neuman@nelsonmullins.com
jeff.kelly@nelsonmullins.com
nate.pencook@nelsonmullins.com
Telephone: 919.329.3800
Facsimile: 919.329.3799

This, the 23rd day of August, 2021.

WOMBLE BOND DICKINSON (US) LLP

/s/ *Ripley Rand*
Ripley Rand
North Carolina State Bar No. 22275
555 Fayetteville Street, Suite 1100
Raleigh, NC 27601
Telephone: (919) 755-8125
Facsimile: (919) 755-6752
Email: ripley.rand@wbd-us.com

Counsel for Plaintiff